

What is claimed is:

1 1. A file management apparatus that encrypts a plaintext
2 to generate a ciphertext, stores the ciphertext, and decrypts
3 the ciphertext, the file management apparatus comprising:
4 a key storage medium storing key information
5 beforehand;

6 registration means for encrypting the key information
7 using a password to generate an encrypted key;

8 encryption means for encrypting a plaintext based on
9 the key information to generate a ciphertext;

10 switch means for switching between (a) generating key
11 information by decrypting the encrypted key using the password
12 and (b) reading the key information from the key storage medium;
13 and

14 decryption means for decrypting the ciphertext based
15 on one of the generated key information and the read key
16 information.

1 2. The file management apparatus of Claim 1 further
2 comprising a memory unit,

3 wherein the registration means receives an input of the
4 password, encrypts the key information using the received
5 password to generate the encrypted key, and writes the
6 generated encrypted key to the memory unit,

7 the encryption means encrypts the plaintext using a file

8 key to generate the ciphertext, encrypts the file key using
9 the key information to generate an encrypted file key, and
10 writes the ciphertext in association with the encrypted file
11 key, to the memory unit,

12 the switch means

13 (a) includes first key obtaining means for receiving
14 an input of the password and decrypting the encrypted key
15 using the received password to generate the key information,
16 and second key obtaining means for reading the key information
17 from the key storage medium, and

18 (b) obtains the key information by one of the first key
19 obtaining means and the second key obtaining means, and

20 the decryption means decrypts the encrypted file key
21 using the obtained key information to generate a file key,
22 and decrypts the ciphertext using the file key to generate
23 a decrypted text.

1 3. The file management apparatus of Claim 2,
2 wherein the registration means further receives an input
3 of a user identifier that identifies a user, and writes the
4 user identifier in association with the encrypted key, to
5 the memory unit, and

6 the first key obtaining means further receives an input
7 of the user identifier and decrypts the encrypted key that
8 is associated with the user identifier.

1 4. The file management apparatus of Claim 2,
2 wherein the registration means further writes the key
3 information and/or authentication information in association
4 with the encrypted key, to the memory unit,
5 the encryption means further writes the encrypted key,
6 the key information, and/or authentication information in
7 association with the ciphertext, to the memory unit,
8 the first key obtaining means checks, using the
9 authentication information, whether the encrypted key has
10 been altered or not, when the encrypted key that is associated
11 with the authentication information is decrypted, and
12 the decryption means checks, using the authentication
13 information, whether the ciphertext has been altered or not,
14 when the ciphertext that is associated with the authentication
15 information is decrypted.

1 5. The file management apparatus of Claim 2,
2 wherein the registration means writes the encrypted key
3 to the memory unit that is a portable storage medium, and
4 the first key obtaining means decrypts the encrypted
5 key that has been written to the memory unit that is the portable
6 storage medium.

1 6. The file management apparatus of Claim 2, further
2 comprising

3 deletion means for deleting the encrypted key that has
4 been written to the memory unit.

1 7. The file management apparatus of Claim 2, further
2 comprising

3 deletion means for deleting the encrypted key that has
4 been written to the memory unit,

5 wherein the registration means further receives an input
6 of a new password, encrypts the key information using the
7 new password to generate a new encrypted key, and writes the
8 generated new encrypted key to the memory unit.

1 8. The file management apparatus of Claim 2,
2 wherein the key storage medium stores new key information
3 beforehand, instead of the key information,

4 the registration means receives the input of the password
5 and decrypts the encrypted key using the password to generate
6 key information,

7 the encryption means decrypts the encrypted file key
8 using the key information to generate a file key, encrypts
9 the file key using the new key information to generate a new
10 encrypted file key, and writes the new encrypted file key
11 over the encrypted file key in the memory unit, and

12 the registration means encrypts the new key information
13 using the password to generate a new encrypted key and writes

14 the new encrypted key over the encrypted key in the memory
15 unit.

1 9. The file management apparatus of Claim 8,
2 wherein the registration means further receives an input
3 of a user identifier that identifies a user,
4 the encryption means further writes the user identifier
5 in association with the ciphertext and the encrypted file
6 key, to the memory unit, and
7 the encryption means retrieves the encrypted file key
8 that is associated with the user identifier in the memory
9 unit and generates a file key from the retrieved encrypted
10 file key.

1 10. The file management apparatus of Claim 8,
2 wherein the encryption means further writes encryption
3 information in association with the ciphertext and the
4 encrypted file key, to the memory unit, the encryption
5 information indicating that the plaintext has been encrypted,
6 and
7 the encryption means retrieves the encrypted file key
8 that is associated with the encryption information in the
9 memory unit, and generates a file key from the retrieved
10 encrypted file key.

11. The file management apparatus of Claim 8,
wherein the registration means further receives an input
of a user identifier that identifies a user,
the encryption means further writes the user identifier
in association with a file identifier that identifies the
ciphertext and the encrypted file key, as a unified file,
to the memory unit, and
the encryption means extracts the file identifier that
is associated with the user identifier from the unified file,
specifies the encrypted file key identified by the extracted
file identifier, and generates a file key from the specified
encrypted file key.

12. The file management apparatus of Claim 8,
wherein the encryption means further writes encryption
information in association with a file identifier that
identifies the ciphertext and the encrypted file key, as a
unified file, to the memory unit, the encryption information
indicating that the plaintext has been encrypted, and
the encryption means extracts the file identifier that
is associated with the encryption information from the unified
file, specifies the encrypted file key identified by the
extracted file identifier, and generates a file key from the
specified encrypted file key.

1 13. The file management apparatus of Claim 2,
2 wherein the encryption means further writes the
3 encrypted key in association with the ciphertext and the
4 encrypted file key, to the memory unit, and
5 the first key obtaining means decrypts the encrypted
6 key that is associated with the ciphertext and the encrypted
7 file key.

1 14. The file management apparatus of Claim 13,
2 wherein the encryption means further receives an input
3 of an indication, the indication showing whether the encrypted
4 key and the ciphertext are to be written in association with
5 each other to the memory unit, and writes, when the indication
6 shows that the encrypted key and the ciphertext are to be
7 written in association with each other, the encrypted key
8 in association with the ciphertext, to the memory unit.

1 15. The file management apparatus of Claim 13,
2 wherein the registration means writes the generated
3 encrypted key to the key storage medium instead of to the
4 memory unit.

1 16. A file encryption apparatus that encrypts a plaintext
2 to generate a ciphertext and stores the ciphertext into a
3 memory unit thereof, the file management apparatus comprising:

4 a key storage medium storing key information
5 beforehand;

6 registration means for receiving an input of a password,
7 encrypts the key information using the received password to
8 generate an encrypted key, and writes the generated encrypted
9 key to the memory unit; and

10 encryption means for encrypting a plaintext using a file
11 key to generate a ciphertext, encrypting the file key using
12 the key information to generate an encrypted file key, and
13 writing the ciphertext in association with the encrypted file
14 key, to the memory unit.

1 17. A file decryption apparatus that stores the
2 ciphertext and the encrypted file key generated by the file
3 encryption apparatus of Claim 16, in association with each
4 other, in a memory unit thereof, and decrypts the ciphertext,
5 the file decryption apparatus comprising:

6 a key storage medium storing key information
7 beforehand;

8 switch means

9 (a) including first key obtaining means for receiving
10 an input of a password and decrypting the encrypted key using
11 the received password to generate key information, and second
12 key obtaining means for reading the key information from the
13 key storage medium, and

14 (b) obtaining the key information by one of the first
15 key obtaining means and the second key obtaining means; and
16 decryption means for decrypting the encrypted file key
17 using the obtained key information to generate a file key,
18 and decrypts the ciphertext using the file key to generate
19 a decrypted text.

1 18. A file management apparatus that encrypts a plaintext
2 to generate a ciphertext, stores the ciphertext, and decrypts
3 the ciphertext, the file management apparatus comprising:
4 a key storage medium storing key information beforehand;
5 registration means for encrypting a password using the
6 key information to generate an encrypted password;
7 encryption means for encrypting a plaintext using a file
8 key to generate a ciphertext, encrypting the file key based
9 on a password obtained by decrypting the encrypted password
10 to generate a first encrypted file key, and encrypting the
11 file key based on the key information to generate a second
12 encrypted file key;
13 switch means for switching between (a) decrypting the
14 first encrypted file key based on the password and (b)
15 decrypting the second encrypted file key based on the key
16 information, to generate a file key; and
17 decryption means for decrypting the ciphertext using
18 the generated file key.

1 19. The file management apparatus of Claim 18 further
2 comprising a memory unit,

3 wherein the registration means receives an input of the
4 password, encrypts the received password using the key
5 information to generate the encrypted password, and writes
6 the generated encrypted password to the memory unit,

7 the encryption means decrypts the encrypted password
8 using the key information to generate the password, encrypts
9 the plaintext using the file key to generate the ciphertext,
10 encrypts the file key using the password to generate the first
11 encrypted file key, encrypts the file key using the key
12 information to generate the second encrypted file key, and
13 writes the ciphertext in association with the first encrypted
14 file key and the second encrypted file key, to the memory
15 unit,

16 the switch means

17 (a) includes first key obtaining means for receiving
18 an input of the password and decrypting the first encrypted
19 file key using the received password, and second key obtaining
20 means for decrypting the second encrypted file key using the
21 key information, and

22 (b) obtains the file key by one of the first key obtaining
23 means and the second key obtaining means, and

24 the decryption means decrypts the ciphertext using the
25 obtained file key to generate a decrypted text.

1 20. The file management apparatus of Claim 19,
2 wherein the registration means further receives an input
3 of a user identifier that identifies a user, and writes the
4 encrypted password in association with the user identifier,
5 to the memory unit, and

6 the encryption means further receives an input of the
7 user identifier and decrypts the encrypted password that is
8 associated with the user identifier.

1 21. The file management apparatus of Claim 19,
2 wherein the encryption means receives an input of an
3 indication, the indication showing whether the first encrypted
4 file key is to be generated or not, and

5 (a) generates, when the indication shows that the first
6 encrypted file key is to be generated, the first encrypted
7 file key, and

8 (b) suppresses, when the indication shows that the first
9 encrypted file key is not to be generated, both generating
10 and writing of the first encrypted file key.

1 22. The file management apparatus of Claim 19,
2 wherein the registration means further writes
3 authentication information in association with the encrypted
4 password, to the memory unit,

5 the encryption means further checks, using the

6 authentication information, whether the encrypted key has
7 been altered or not, when the encrypted key is decrypted,
8 and

9 the encryption means further writes the authentication
10 information in association with each of the first encrypted
11 file key, the second encrypted file key, and the ciphertext,
12 to the memory unit,

13 the first key obtaining means and the second key obtaining
14 means each check, using the authentication information
15 associated with the first encrypted file key and the second
16 encrypted file key, whether the first encrypted file key and
17 the second encrypted file key have been altered or not, when
18 the first encrypted file key and the second encrypted file
19 key are decrypted, and

20 the decryption means checks, using the authentication
21 information that is associated with the ciphertext, whether
22 the ciphertext has been altered or not, when the ciphertext
23 is decrypted.

1 23. The file management apparatus of Claim 19,
2 wherein the registration means writes the encrypted
3 password to the key storage medium, instead of to the memory
4 unit, and

5 the encryption means decrypts the encrypted password
6 that has been written to the key storage medium.

1 24. The file management apparatus of Claim 19,
2 wherein the registration means further receives an input
3 of a new password, encrypts the new password using the key
4 information to generate a new encrypted password, and writes
5 the generated new encrypted password over the encrypted
6 password in the memory unit, and

7 the encryption means decrypts the second encrypted file
8 key using the key information to generate a file key, encrypts
9 the file key using the new password to generate a new first
10 encrypted file key, and writes the new first encrypted file
11 key over the first encrypted file key in the memory unit.

1 25. The file management apparatus of Claim 24,
2 wherein the registration means further receives an input
3 of a user identifier that identifies a user,

4 the encryption means further writes the user identifier
5 in association with the ciphertext, the first encrypted file
6 key, and the second encrypted file key, to the memory unit,
7 and

8 the encryption means retrieves the second encrypted file
9 key that is associated with the user identifier, and decrypts
10 the retrieved second encrypted file key.

11

1 26. The file management apparatus of Claim 24,
2 wherein the encryption means further writes encryption

3 information in association with the ciphertext, the first
4 encrypted file key, and the second encrypted file key, to
5 the memory unit, the encryption information indicating that
6 the plaintext has been encrypted, and

7 the encryption means retrieves the second encrypted file
8 key that is associated with the encryption information, and
9 decrypts the retrieved second encrypted file key.

10

1 27. The file management apparatus of Claim 24,
2 wherein the registration means further receives an input
3 of a user identifier that identifies a user,

4 the encryption means further writes the user identifier
5 in association with a file identifier that identifies the
6 ciphertext, the first encrypted file key, and the second
7 encrypted file key, as a unified file, to the memory unit,
8 and

9 the encryption means extracts the file identifier that
10 is associated with the user identifier from the unified file,
11 specifies the second encrypted file key identified by the
12 extracted file identifier, and decrypts the specified second
13 encrypted file key.

1 28. The file management apparatus of Claim 24,
2 wherein the encryption means further writes encryption
3 information in association with a file identifier that

4 identifies the ciphertext, the first encrypted file key, and
5 the second encrypted file key, as a unified file, to the memory
6 unit, the encryption information indicating that the plaintext
7 has been encrypted, and

8 the encryption means extracts the file identifier that
9 is associated with the encryption information from the unified
10 file, specifies the second encrypted file key identified by
11 the extracted file identifier, and generates a file key from
12 the specified second encrypted file key.

1 29. The file management apparatus of Claim 19 further
2 comprising

3 deleting means for deleting the second encrypted file
4 key that has been written to the memory unit.

1 30. The file management apparatus of Claim 19,
2 wherein the key storage medium stores new key information
3 beforehand, instead of the key information,

4 the registration means receives the input of the password
5 and decrypts the received password using the new key
6 information to generate a new encrypted password, and writes
7 the generated new encrypted password over the encrypted
8 password in the memory unit, and

9 the encryption means decrypts the first encrypted file
10 key using the password to generate a file key, encrypts the

11 file key using the new key information to generate a new second
12 encrypted file key, and writes the new second encrypted file
13 key over the second encrypted file key in the memory unit.

1 31. The file management apparatus of Claim 30,
2 wherein the registration means further receives an input
3 of a user identifier that identifies a user,
4 the encryption means further writes the user identifier
5 in association with the ciphertext, the first encrypted file
6 key, and the second encrypted file key, to the memory unit,
7 the encryption means retrieves the first encrypted file
8 key that is associated with the user identifier and decrypts
9 the retrieved first encrypted file key.

1 32. The file management apparatus of Claim 30,
2 wherein the encryption means further writes encryption
3 information in association with the ciphertext, the first
4 encrypted file key, and the second encrypted file key, to
5 the memory unit, the encryption information indicating that
6 the plaintext has been encrypted, and
7 the encryption means retrieves the first encrypted file
8 key that is associated with the encryption information and
9 decrypts the retrieved first encrypted file key.

1 33. The file management apparatus of Claim 30,

2 wherein the registration means further receives an input
3 of a user identifier that identifies a user,

4 the encryption means further writes the user identifier
5 in association with a file identifier that identifies the
6 ciphertext, the first encrypted file key, and the second
7 encrypted file key, as a unified file, to the memory unit,
8 and

9 the encryption means extracts the file identifier that
10 is associated with the user identifier from the unified file,
11 specifies the first encrypted file key identified by the
12 extracted file identifier, and decrypts the specified first
13 encrypted file key.

1 34. The file management apparatus of Claim 30,

2 wherein the encryption means further writes encryption
3 information in association with a file identifier that
4 identifies the ciphertext, the first encrypted file key, and
5 the second encrypted file key, as a unified file, to the memory
6 unit, the encryption information indicating that the plaintext
7 has been encrypted, and

8 the encryption means extracts the file identifier that
9 is associated with the encryption information from the unified
10 file, specifies the first encrypted file key identified by
11 the extracted file identifier, and generates a file key from
12 the specified first encrypted file key.

1 35. The file management apparatus of Claim 19,
2 wherein the switch means further receives an input of
3 the password, decrypts the first encrypted file key using
4 the received password to generate a first file key, decrypts
5 the second encrypted file key using the key information to
6 generate a second file key, judges whether the first file
7 key and the second file key match, and detects an error when
8 the first file key and the second file key do not match.

1 36. A file encryption apparatus that encrypts a plaintext
2 to generate a ciphertext and stores the ciphertext in a memory
3 unit thereof, the file encryption apparatus comprising:

4 a key storage medium storing key information beforehand;
5 registration means for receiving an input of a password,
6 encrypts the received password using the key information to
7 generate an encrypted password, and writes the generated
8 encrypted password to the memory unit; and

9 encryption means for decrypting the encrypted password
10 using the key information to generate a password, encrypts
11 a plaintext using a file key to generate a ciphertext, encrypts
12 the file key using the password to generate a first encrypted
13 file key, encrypts the file key using the key information
14 to generate a second encrypted file key, and writes the
15 ciphertext in association with the first encrypted file key
16 and the second encrypted file key, to the memory unit.

1 37. A file decryption apparatus that stores the
2 ciphertext, the first encrypted file key, and the second
3 encrypted file key generated by the file encryption apparatus
4 of Claim 35, in association with each other, in a memory unit
5 thereof, and decrypts the ciphertext, the file decryption
6 apparatus comprising:

7 a key storage medium storing key information beforehand;
8 switch means

9 (a) including first key obtaining means for receiving
10 an input of a password and decrypting the first encrypted
11 file key using the received password, and second key obtaining
12 means for decrypting the second encrypted file key using the
13 key information, and

14 (b) obtaining a file key by one of the first key obtaining
15 means and the second key obtaining means, and

16 decryption means for decrypting the ciphertext using
17 the obtained file key to generate a decrypted text.